Reg.No.:												

VIVEKANANDHA COLLEGE OF ENGINEERING FOR WOMEN
[AUTONOMOUS INSTITUTION AFFILIATED TO ANNA UNIVERSITY, CHENNAI]
Elayampalayam – 637 205, Tiruchengode, Namakkal Dt., Tamil Nadu.

Question Paper Code: 6013

B.E. / B.Tech. DEGREE END-SEMESTER EXAMINATIONS – MAY / JUNE 2024
Sixth Semester
Information Technology
U19ITV23 – CYBER FORENSICS
(Common to CSE)
(Regulation 2019)

Time: Three Hours | Maximum: 100 Marks

Answer ALL the questions

Knowledge Levels (KL)	K1 – Remembering	K3 – Applying	K5 - Evaluating
	K2 – Understanding	K4 – Analyzing	K6 - Creating

PART – A

(10 x 2 = 20 Marks)

Q.No.	Questions	Marks	KL	CO
1.	List the steps involved in assessing the digital evidence in a computer investigation.	2	K3	CO1
2.	Highlight one challenge associated with handling digital evidence.	2	K2	CO1
3.	What are the steps involved in setting up and utilizing write-protection for USB devices in a Windows XP system?	2	K2	CO2
4.	Mention the scenario where knowledge of storage formats influenced the outcome of a digital forensic investigation.	2	K3	CO2
5.	Provide an example of digital evidence commonly encountered in cybercrime cases.	2	K1	CO3
6.	What are the steps to create image files of digital evidence?	2	K2	CO3
7.	Mention the roles of computer forensics software tools in digital investigations.	2	K1	CO4
8.	List the importance of validating and testing forensic software tools.	2	K3	CO4
9.	Mention the methods used in identifying unknown file formats during digital forensic analysis.	2	K4	CO5

10.	Differentiate between copyright infringement and fair use.	2	K2	CO5

PART – B

(5 x 13 = 65 Marks)

Q.No.		Questions	Marks	KL	CO
11.	a)	Discuss the challenges associated with presenting digital evidence in legal proceedings. How can investigators prepare to address these challenges and ensure the admissibility of the evidence in court?	13	K2	CO1
		(OR)			
	b)	Provide an example of a complex computer investigation and discuss the strategies employed to overcome challenges and achieve a successful outcome.	13	K3	CO1
12.	a)	Discuss the factors that investigators should consider when determining the best acquisition method for digital evidence. Provide two examples of situations where different acquisition methods might be appropriate.	13	K3	CO2
		(OR)			
	b)	Discuss the benefits and risks of using remote network acquisition tools in digital forensics. How can investigators ensure the security and integrity of the acquired data in a remote acquisition scenario?	13	K3	CO2
13.	a)	Explain the differences between collecting digital evidence in private sector incident scenes and law enforcement crime scenes. Provide two considerations unique to private sector incidents.	13	K4	CO3
		(OR)			
	b)	Discuss the challenges associated with seizing digital evidence at the scene. How can investigators ensure the proper collection and preservation of digital evidence during the seizure process?	13	K3	CO3
14.	a)	Discuss about			
		i. Hardware and software forensics tools.	8	K2	CO4
		ii. Validating forensic software.	5		
		(OR)			
	b)	Describe the process of determining data collection and analysis in computer forensics. How does this decision-making phase impact the overall success of a forensic investigation?	13	K3	CO4

15.	a)	Discuss key security considerations for email servers in the context of forensic investigations. How can a compromised email server affect the integrity of digital evidence?	13	K3	CO5
		(OR)			
	b)	Discuss how data compression techniques can affect the recognition and recovery of graph files. Outline techniques for recovering graph files that have undergone compression.	13	K2	CO5

PART – C

(1 x 15 = 15Marks)

Q.No.		Questions	Marks	KL	CO
16	a)	Discuss challenges that may arise during the investigation and propose solutions for overcoming them. Determine and justify the best acquisition method for corporate high-tech investigation.	15	K4	CO2
		(OR)			
	b)	Explain the considerations and procedures involved in performing remote acquisitions. Discuss the ethical and legal implications of remote acquisitions in the context of this investigation.	15	K3	CO4